Department of Homeland Security Daily Open Source Infrastructure Report for 29 June 2007

Current Nationwide Threat Level is ELEVATED
Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- The Associated Press reports the wing of a departing jetliner struck the tail of another plane on a holding pad at Chicago's O'Hare International Airport on Wednesday, June 27, during a severe thunderstorm. (See item 13)
- The New York Times reports tainted Chinese toothpaste was widely distributed in the U.S., with roughly 900,000 tubes turning up in hospitals for the mentally ill, prisons, juvenile detention centers, and even some hospitals serving the general population. (See item 23)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *June 28, Associated Press* — **Blackout causes chaos in New York City, but power is restored quickly.** As energy officials investigated what caused a brief blackout that darkened a large swath of Manhattan and the Bronx, New York on Thursday, June 28, faced another day of extreme heat and possible thunderstorms. Consolidated Edison Chief Executive Kevin Burke said lightning may have caused Wednesday's blackout; there were severe thunderstorms in the area around that time. Wednesday's blackout lasted less than an hour. But it recalled some of the confusion the city endured during blackouts last year and in 2003, and left some residents wondering whether it was a sign of trouble to come. The outage knocked out traffic lights and

snarled subway service. The blackout affected approximately 385,000 people, Burke said Wednesday. The outage began at 3:42 p.m. EDT and all power was restored by 4:30 p.m., Burke said. He strove to reassure New Yorkers that the "likelihood of this happening again is very low." Burke said energy consumption did not cause the blackout. The problem Wednesday started in a Queens substation that is connected to two others in the Bronx and Upper East Side, Burke said.
Source: http://cityroom.blogs.nytimes.com/2007/06/27/power−dip−disrupts−east−side−subway−service/

2. *June 28, Reuters* — **Oil price−demand link no longer as simple as ABC.** "Oil prices go up and demand goes down, it's simple, it's ABC," then Saudi Oil Minister Zaki Yamani was quoted as saying in 1979, shortly before demand then prices collapsed from a record above $30 a barrel. Few would agree with him today. Oil above $60 for the best part of two years and at $70 now has barely dented demand growth and neither the Organization of the Petroleum Exporting Countries (OPEC) nor the International Energy Agency (IEA) foresee a repeat of the events of 1979−1983, when consumption fell sharply. "We have seen unprecedented economic growth in the past 2−3 years, unaffected by oil prices," said Hasan Qabazard of OPEC. Lawrence Eagles of IEA said, "The primary driver of oil demand is GDP growth and not prices. And as world moves towards a more transportation fuel oriented model these rigidities become more entrenched." Despite the best efforts of policymakers in the United States and Europe, there is no "quick fix" for the world's addiction to gasoline and diesel.
Source: http://www.signonsandiego.com/news/business/20070628−0714−oil−demand.html

3. *June 27, Reuters* — **Electric utilities to study new solar technology.** The Electric Power Research Institute said on Wednesday, June 27, it will launch a project to study the feasibility of "concentrating" solar power to increase its efficiency at the request of a number of western U.S. electric utilities. Unlike conventional flat−plate solar or photovoltaic panels, concentrating solar power uses reflectors to generate electricity more efficiently and in larger amounts, EPRI said. The institute said the project will study the feasibility of building a solar power plant in the 50− to 500−megawatt range, much larger than traditional solar installations. The industry research group said the United States has four such utility−size solar plants: one in Nevada and three in California. EPRI said the solar project was initiated by New Mexico−based PNM Resources Inc. which is interested in building such a solar facility in New Mexico by 2010. Other utilities that will participate in the study's first phase include San Diego Gas & Electric, Southern California Edison, Tri−State Generation and Transmission Association and Xcel Energy. El Paso Electric has also expressed interest in the project, EPRI said.
Source: http://today.reuters.com/news/articlenews.aspx?type=scienceNews&storyID=2007−06−27T173847Z_01_N27299054_RTRUKOC_0_US−UTILITIES−SOLAR−EPRI.xml

4. *June 27, Associated Press* — **NRC updating plant safety requirements.** The Nuclear Regulatory Commission (NRC) on Wednesday, June 27, took the first step in updating the operating licenses of the nation's nuclear plants to ensure they incorporate safety rules issued after the September 11 attacks. NRC issued letters to FirstEnergy Corp.'s Beaver Valley plant in Pennsylvania, Exelon Corp.'s Braidwood and Byron generating stations in Illinois, Ameren Corp.'s Callaway plant in Missouri, and Progress Energy's H.B. Robinson plant in South Carolina. Letters to the operators of the nation's remaining 96 operating reactors will be issued

over the next two months. All nuclear power plants must now be prepared to mitigate the effects of large fires and explosions from a terrorist attack, including the impact of a large commercial aircraft. The NRC said most of the measures being required through revised plant operating licenses are already in place and have been verified by the agency. The updated requirements will become part of the routine inspections at all operating reactors.
Source: http://www.forbes.com/feeds/ap/2007/06/27/ap3864652.html

[Return to top]

Chemical Industry and Hazardous Materials Sector

5. *June 27, 9 News (CO)* — **Businesses evacuated due to chemical spill.** A hydrochloric acid leak at a business forced closures and evacuations Wednesday morning, June 27, to allow crews to clean up. Castle Rock, CO, Police say the leak occurred at Pure Water Solutions, located at 520 Topeka Way. Police say the business owner suspects about 200 gallons of hydrochloric acid spilled inside the business. As a precaution, authorities evacuated a 300−foot radius surrounding the building. Included in the evacuations was Air Care Colorado's nearby vehicle emissions testing station, located at 541 Topeka Way.
Source: http://www.9news.com/news/article.aspx?storyid=72708

[Return to top]

Defense Industrial Base Sector

6. *June 28, Government Accountability Office* — **GAO−07−620: Defense Acquisitions: An Analysis of the Special Operations Command's Management of Weapon System Programs (Report).** Special Operations Command's (SOCOM) duties have greatly increased since the attacks of September 11, 2001. Today, Special Operations Forces are at work in Afghanistan and Iraq, and SOCOM has been assigned to lead U.S. efforts in the Global War on Terrorism. SOCOM's acquisitions budget has also greatly increased in this period −− more than doubling from $788 million in 2001 to approximately $1.91 billion in 2006. In light of SOCOM's expanded duties, Congress requested that the Government Accountability Office (GAO) review SOCOM's management of its acquisition programs. GAO's evaluation includes an assessment of: the types of acquisition programs SOCOM has undertaken since 2001 and whether the programs are consistent with its mission; the extent to which SOCOM's programs have progressed as planned; and the challenges SOCOM faces in managing its acquisition programs. GAO recommends that the Secretary of Defense take steps to ensure SOCOM (1) establishes sound business cases when starting programs, particularly its more complex and department−managed programs; (2) has the workforce size and composition to match its acquisition workload; and (3) improves its acquisition management information system. The Department of Defense generally concurred with these recommendations.
Highlights: http://www.gao.gov/highlights/d07620high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−07−620

[Return to top]

Banking and Finance Sector

7. *June 28, IDG News Service* — **DOJ warns U.S. citizens of phishing attack.** The U.S. Department of Justice (DOJ) is alerting e−mail users about a possible phishing attack using messages that claim to be from the DOJ. In a news release Thursday, June 28, the DOJ said the e−mails may have the subject field or be addressed "Dear Citizen." It also said the messages may refer to a fraudulent U.S. Internal Revenue Service case filed against the recipient, and may contain a DOJ logo in the body of the mail or as an attachment. The DOJ said the e−mail is a hoax.
   Source: http://www.infoworld.com/article/07/06/28/DOJ−warns−of−phish ing−attack_1.html

8. *June 28, CNET News* — **eBay targets Romanian scammers.** eBay has made public the details of a months−long campaign to curb online fraud arising in Romania −− an effort that has resulted in several hundred arrests. The e−commerce site's internal fraud team first took note of a higher−than−usual amount of fraudulent activity from Eastern Europe in 2005. While schemes varied, many of the suspects set out to commit fraud after approaching eBay users who had narrowly lost an auction. "The scammer can see that a user that didn't win was prepared to spend $145 on a particular item," said Matt Henley of eBay's Fraud Investigations Team. "They would then attempt to contact the user off the eBay platform to offer them a second chance." The scammers would first have to guess the e−mails of the losing bidders −− most commonly by combining their eBay username with popular Web−mail domains. "It's very common that users have the same username for their eBay as their e−mail," Henley explained. The would−be scammers would have a certain level of success, he said, "simply by sending out 50 e−mails of the most common domain names −− including the eBay user name at Gmail, Hotmail, Yahoo."
   Source: http://news.com.com/eBay+targets+Romanian+fraudsters/2100−73 48_3−6193591.html

9. *June 28, InformationWeek* — **Hackers make off with personal info on applicants at University of California−Davis.** The University of California−Davis (UC−Davis) Police Department and Sacramento Valley High Tech Crimes Task Force are investigating the possible theft and misuse of records containing information on about 1,120 aspiring veterinarians who'd applied to UC−Davis School of Veterinary Medicine for the school year starting this fall. Law enforcement was alerted to the intrusion on June 15, after applicants admitted into the School of Veterinary Medicine attempted to set up campus computer accounts but were notified that accounts had already been established in their names. This led law enforcement to discover that the records of 375 veterinary medical school applicants for the 2004−2005 school year also might have been compromised. Even professionals who long ago traded in their books for briefcases aren't safe. Bowling Green State University is notifying current and former students of a certain accounting professor that a computer flash drive with information about them has been lost. Files on the portable storage device contained Social Security numbers for 199 students from the professor's classes in 1992, and the names, grades, and university identification numbers −− although not the Social Security numbers −− for about another 1,600 other students.
   Source: http://www.informationweek.com/security/showArticle.jhtml;js essionid=A1PK5RAA5NNU0QSNDLPCKHSCJUNN2JVN?articleID=20000137 4&articleID=200001374

10. *June 27, Reuters* — **Canada outlines tougher money−laundering rules.** Canadian financial institutions and intermediaries will have to strengthen their reporting of suspected money−laundering transactions, and bear the extra cost, according to new rules published on Wednesday, June 27. Changes to the anti−money−laundering and anti−terrorist financing regulations, mean some financial firms must now report to authorities any "attempted suspicious transactions," in addition to actual ones. Certain institutions must also gather more detailed data on certain clients and business partners, including large corporate shareholders and foreign banks, and politically exposed individuals. Ottawa also fleshed out requirements for foreign exchange dealers to register with Canada's financial intelligence unit, FINTRAC. Under the regulations, first drafted after the September 11, 2001, attacks on the United States, banks and other financial institutions and brokers have to report all large cash transactions or electronic fund transfers of $9,300 or more. They must also report any transaction they have reasonable grounds to suspect is related to terrorist financing or money−laundering. The new measures also allow FINTRAC to share more personal information on suspects of financial crime, such as phone number and address, with the police and intelligence agencies.
Source: http://ca.today.reuters.com/news/newsArticle.aspx?type=domesticNews&storyID=2007−06−27T172359Z_01_N27411044_RTRIDST_0_CANADA−FINANCIAL−REGULATIONS−COL.XML

11. *June 26, Computerworld New Zealand* — **New Zealand banks demand a peek at customer PCs in fraud cases.** Banks in New Zealand are seeking access to customer PCs used for online banking transactions to verify whether they have enough security protection. Under the terms of a new banking Code of Practice, banks may request access in the event of a disputed transaction to see if security protection in is place and up to date. The code, issued by the Bankers' Association last week after lengthy drafting and consultation, now has a new section dealing with Internet banking. Liability for any loss resulting from unauthorized Internet banking transactions rests with the customer if they have "used a computer or device that does not have appropriate protective software and operating system installed and up−to−date, [or] failed to take reasonable steps to ensure that the protective systems, such as virus scanning, firewall, antispyware, operating system and antispam software on [the] computer, are up−to−date." The code also adds: "We reserve the right to request access to your computer or device in order to verify that you have taken all reasonable steps to protect your computer or device and safeguard your secure information in accordance with this code...If you refuse our request for access then we may refuse your claim."
Source: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9025780&intsrc=news_list

[Return to top]

Transportation and Border Security Sector

12. *June 28, Government Accountability Office* — **GAO−07−1044T: Homeland Security: Prospects For Biometric US−VISIT Exit Capability Remain Unclear (Testimony).** The Department of Homeland Security (DHS) has spent and continues to invest hundreds of millions of dollars each year in its U.S. Visitor and Immigrant Status Indicator Technology (US−VISIT) program to collect, maintain, and share information on selected foreign nationals who enter and exit the United States at over 300 air, sea, and land ports of entry (POEs). The

program uses biometric identifiers (digital finger scans and photographs) to screen people against watch lists and to verify that a visitor is the person who was issued a visa or other travel document. The Government Accountability Office's (GAO) testimony addresses the status of US−VISIT entry and exit capabilities and DHS's management of past and future exit efforts. In developing its testimony, GAO drew from eight prior reports on US−VISIT as well as ongoing work for the committee. In light of the department's longstanding challenges in delivering an operational exit capability and the uncertainty surrounding its future exit efforts, GAO urges the department to approach its latest attempt at deploying mission critical exit capabilities with the kind of rigor and discipline that GAO has previously recommended.
Highlights: http://www.gao.gov/highlights/d071044thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−07−1044T

13. *June 28, Associated Press* — **Planes touch on ground at Chicago−O'Hare.** The wing of a departing jetliner struck the tail of another plane on a holding pad at O'Hare International Airport during a severe thunderstorm, authorities said. No injuries or fuel spills were reported. Chicago Department of Aviation spokesperson Wendy Abrams said the accident occurred about 3:50 p.m. Wednesday, June 27, when the wing of a taxiing United Airlines B777 struck the tail of a stationary American Airlines MD80. The United plane appeared undamaged and taxied back to the gate a short time after the collision, but American spokesperson Mary Frances Fagan said the American plane suffered damage to its rudder and remained on the holding pad for about an hour before returning to the gate. Fagan said American Flight 1817 was carrying 136 passengers and five crewmembers and had been scheduled to depart for Seattle. United spokesperson Jeff Kovick said United Flight 149, bound for San Francisco, was carrying 347 passengers and a crew of 11. Tony Molinaro of the Federal Aviation Administration said his agency was investigating the accident and had notified the National Transportation Safety Board. Molinaro said aircraft operators are responsible for maintaining their distance from one another on the holding pad.
Source: http://biz.yahoo.com/ap/070628/il_planes_collide.html?.v=1

14. *June 27, Associated Press* — **Qatar Airways, United to apply for Codeshare.** Qatar Airways said Wednesday, June 27, it will file a joint application with United Airlines to form a code sharing partnership, which will allow each carrier to sell seats on the other's planes. Such partnerships effectively broaden the reach of each airline's route network, as customers can buy a single ticket and check in at one carrier's desk but then fly legs on both airlines' planes. Qatar Airways began servicing the United States this week with a flight from its Doha base to Newark, NJ. It plans to begin a flight to Washington, DC, where United has a hub at Dulles International Airport, on July 19.
Source: http://biz.yahoo.com/ap/070627/qatar_united.html?.v=1

15. *June 27, Boston Globe* — **Police stop, search Boston's Red Line train after alleged threats.** Police arrested a man on the Massachusetts Bay Transportation Authority's (MBTA) Red Line who was accused of threatening to blow up a train with a bomb. A passenger on the train used a cell phone to report the threat to MBTA police, who arrested Troy Norman, 18, at Wollaston Station at about 10 a.m., Lieutenant Commander Joseph O'Connor said. The special operations unit for the MBTA searched the train but did not find any weapons or explosives, O'Connor said. Service resumed in a half hour. Norman, of Quincy, was taken to MBTA police headquarters and booked on a charge of making threats, O'Connor said.

Source: http://www.boston.com/news/globe/city_region/breaking_news/2007/06/police_stop_sea.html

16. *June 27, Miami Herald* — **MIA gate evacuated after powder found.** Security workers evacuated a portion of Miami International Airport's (MIA) A Concourse Wednesday night, June 27, after a powdery substance was found aboard an American Airlines plane departing for Peru. Police dogs did not indicate a threat from the powder, but a bomb squad was checking the area about 9 p.m. EDT to be sure, Transportation Security Administration spokesperson Sari Koshetz said. American Flight 917 was scheduled to depart from Miami to Lima's Chavez International Airport. It was parked at gate A10 at Miami International when the suspicious substance was discovered. The plane and surrounding gate area were evacuated as investigators checked things out.
Source: http://www.miamiherald.com/news/breaking_dade/story/153594.h tml

[Return to top]

Postal and Shipping Sector

17. *June 28, Associated Press* — **FedEx expands service in China.** Package−delivery company FedEx Corp.'s FedEx Express unit on Thursday, June 28, said its next−business−day service is now available to customers in China. FedEx began next−business−day service in the country on May 28 and now services 30 cities. The company said its 48−hour day−definite service is offered in more than 200 cities and counties in China.
Source: http://biz.yahoo.com/ap/070628/fedex_product.html?.v=1

18. *June 28, Associated Press* — **Kansas City: Powder shuts down IRS mailroom, bomb clears Liberty City Hall.** The Kansas City area dealt with two scares on Wednesday, June 27, with a suspicious white powder found in an Internal Revenue Service mailroom, and what authorities called a pipe bomb −− filled with fireworks sparklers −− found in the Liberty, MO, City Hall. A letter containing a white powder and a note mentioning anthrax forced federal authorities to shut down the mailroom of the Kansas City IRS headquarters. The letter was sealed and sent to a lab in Jefferson City, MO, for further testing, said FBI spokesperson Bob Herndon. A mailroom employee who handled the letter went through decontamination procedures, Herndon said. He said the mailroom was being sealed off until the test results came back late Wednesday or early today. The facility has a different ventilation system from the rest of the IRS headquarters. Herndon refused to comment on earlier reports that the letter had a return address of a state prison, other than to say investigators were following a "viable lead" to the letter's sender. Meanwhile, workers were evacuated from the Liberty City Hall for about two hours while an explosives squad destroyed a pipe bomb.
Source: http://www.stltoday.com/stltoday/news/stories.nsf/missouristatenews/story/48CF6442CB06983C86257308000F7877?OpenDocument

19. *June 27, Associated Press* — **Postal workers charged with stealing ATM cards.** Worcester County, MD, authorities have charged a postal worker with stealing credit and ATM cards from the mail. The Worcester Bureau of Investigation arrested 26−year−old Nikhik Girishbhai Patel of Salisbury, MD, last week and charged him with 36 counts of credit card theft and fraud

charges. Court documents state Patel used the cards to withdraw cash from banks and make store purchases. Police say Patel stole about $3,000 from six victims.
Source: http://wjz.com/local/local_story_178085748.html

[Return to top]

Agriculture Sector

20. *June 27, Associated Press* — **Experts: crawfish disease maybe not as bad as feared.** A crawfish virus first detected in May has been confirmed in ponds throughout south Louisiana, but researchers said it might not be as destructive as initially feared. White spot disease can be deadly to crustaceans. The disease has now been documented in wild crawfish from the Atchafalaya Basin and in 62 out of 94 ponds with completed test results. The Louisiana State University Agricultural Center said tests have confirmed the virus in ponds in 11 parishes, including most of the Acadiana region and Iberville and East Baton Rouge parishes. Aquaculture specialist Greg Lutz said less than one−tenth of the infected ponds have experienced significant crawfish deaths.
Source: http://www.wdsu.com/news/13578985/detail.html

21. *June 27, Akron Beacon Journal (OH)* — **Cucumber crop threatened by mildew.** A potentially devastating mildew has been found on cucumber farms in northern Ohio. The downy mildew was confirmed in a cucumber field in Medina County on June 21 and in Erie County on June 25, reported Sally Miller, a plant pathologist with the Ohio Agricultural Research and Development Center. Officials do not know the source of the spores that triggered the Ohio outbreak. The spores are found in the winter in Mexico and southern states. The fungus can be carried north by winds or storms, but Miller said the outbreak could be from greenhouse production in Canada. Last year, the disease hit cucumber farms in Ohio and Michigan and cost growers millions of dollars in lost crops and fungicide costs.
Source: http://www.ohio.com/mld/beaconjournal/17425446.htm

22. *June 26, Pittsburgh Tribune−Review* — **'Devastating' beetle spreads to Pennsylvania.** State and federal agricultural officials confirmed Tuesday, June 26, that a beetle responsible for killing more than 20 million ash trees in five states has surfaced in Western Pennsylvania. The U.S. Department of Agriculture positively identified the emerald ash borer (EAB) in Cranberry. No further details have been released. The beetle first appeared in North America five years ago, taking hold in southeastern Michigan. Native to eastern Russia and Asia, officials suspect it was transported to the U.S. by cargo ships in the Great Lakes. Since then, states with EAB infestations have imposed quarantines and fines for transporting wood, and cut down trees in an attempt to stem the spread of the ash borer. Because the beetle does not have a natural predator in the U.S., it spreads easily. It also has surfaced in Ohio, Indiana, Illinois and Maryland.
EAB information: http://www.emeraldashborer.info/
Source: http://www.pittsburghlive.com/x/pittsburghtrib/s_514523.html

[Return to top]

Food Sector

23. *June 28, New York Times* — **Wider sale is seen for toothpaste tainted in China.** After federal health officials discovered last month that tainted Chinese toothpaste had entered the U.S., they warned that it would most likely be found in discount stores. In fact, the toothpaste has been distributed much more widely. Roughly 900,000 tubes containing a poison used in some antifreeze products have turned up in hospitals for the mentally ill, prisons, juvenile detention centers and even some hospitals serving the general population. The toothpaste was handed out in dozens of state institutions, mostly in Georgia but also in North Carolina, according to state officials. Hospitals in South Carolina and Florida also reported receiving Chinese−made toothpaste, and a major national pharmaceutical distributor said it was recalling tainted Chinese toothpaste. State officials in Georgia and North Carolina said all the tainted tubes were being replaced with brands made outside China. Since the Panamanian government found Chinese toothpaste with diethylene glycol in May, countries from Latin America to West Africa to Japan have seized the toothpaste. Panama last year inadvertently mixed the poison made in China into 260,000 bottles of cold medicine, killing at least 100 people, prosecutors there said.
Source: http://www.nytimes.com/2007/06/28/us/28tooth.html?ei=5090&en=a00a39144f0b11b4&ex=1340683200&partner=rssuserland&emc=rss& pagewanted=print

24. *June 27, Patriot−News (PA)* — **Candy producer probes contamination incident.** What happened at The Hershey Co. plant in Derry, PA, last week? "We had a product issue at the plant last week," Hershey spokesperson Kirk Saville said Tuesday, June 26. "The system isolated it and no product involved left the plant. We are investigating the issue." Dennis Bomberger, business manager for the Chocolate Workers union local at the plant, said employees did everything they were supposed to do once the contamination was discovered. He said production had to be shut down for a time. "I'm here 40 years, and it's not the first time the wrong product got in the wrong machine," Bomberger said.
Source: http://www.pennlive.com/business/patriotnews/index.ssf?/base/business/1182905726249430.xml&coll=1

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

25. *June 28, Agence France−Presse* — **Pakistan to launch world's biggest anti−measles drive.** Pakistani authorities and United Nations agencies said Thursday, June 28, they will immunize 63 million children against measles in the biggest such campaign in history. The virulent disease is one of the deadliest threats to young people in Pakistan, claiming the lives of 58 children a day, but vaccination coverage there is currently only 69 percent. The campaign targeting all children aged up to 13 years is due to start on Monday, July 2, in southwestern Baluchistan province. It will cover the whole country by March 2008, officials said. Around one million Pakistani children catch measles every year and nearly 21,000 die from it. Measles

was the world's single most lethal infectious disease before an effective vaccine emerged in 1963.
Source: http://news.yahoo.com/s/afp/20070628/hl_afp/healthpakistanunmeasles_070628134343;_ylt=AnQdeWp_NvGm_rY3CR5eMH.JOrgF

26. *June 27, Associated Press* — **United Nations finds progress in tackling bird flu.** Countries are making progress in fighting bird flu but concerns remain for some nations −− especially Indonesia, Egypt and Nigeria −− where human contamination is still possible, the United Nations said Wednesday, June 27. Scientists and officials gathering in Rome, Italy, for a three−day technical meeting on bird flu said that in most cases the virus is rapidly detected and kept under control, as most countries are equipped with improved response systems. However, in nations that combine a high density of population and unsafe poultry management, the situation remains serious. Joseph Domenech, the chief veterinary officer of the UN Food and Agriculture Organization, said Domenech said that Indonesia presents the highest danger due to the great number of people having direct contact with poultry. Indonesia has more than 13,000 live poultry markets where birds of different origins are mixed.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2007/06/27/AR2007062700911.html

27. *June 27, Xinhua (China)* — **China to establish anti−bioterrorism system.** China will make efforts to establish a biological security system in 20 years to fight against bioterrorism and prevent serious epidemic diseases, according to a report released by the Ministry of Science and Technology (MOST) on Tuesday, June 26. The report, issued at the International Biological Economy Meeting held in Tianjin, said by the end of 2007, China will develop vaccines and medicines for genes used in bioterrorism and the physical protective technology and equipment, and establish a monitoring network over bio−terrorism. A research center to exam and prevent serious epidemic diseases will also be established, according to the report.
Source: http://news.xinhuanet.com/english/2007−06/27/content_6295537.htm

28. *June 26, PLoS Medicine* — **An epidemiological network model for disease outbreak detection.** Advanced disease−surveillance systems have been deployed worldwide to provide early detection of infectious disease outbreaks and bioterrorist attacks. New methods that improve the overall detection capabilities of these systems can have a broad practical impact. Most current generation surveillance systems are vulnerable to dramatic and unpredictable shifts in the health−care data that they monitor. These shifts can occur during major public events as a result of population surges and public closures. Shifts can also occur during epidemics and pandemics as a result of quarantines, the worried−well flooding emergency departments or, conversely, the public staying away from hospitals for fear of nosocomial infection. As a result, public−health crises and major public events threaten to undermine health−surveillance systems at the very times they are needed most. Researchers introduced a class of epidemiological network models that monitor the relationships among different health−care data streams instead of monitoring the data streams themselves. Researchers evaluated the models effectiveness using historical emergency department data. The results show that the network models provide better detection of localized outbreaks, and greater robustness to unpredictable shifts than a reference time−series modeling approach.
Source: http://medicine.plosjournals.org/archive/1549−1676/4/6/pdf/10.1371_journal.pmed.0040210−L.pdf

29. *June 21, Independent (South Africa)* — **XDR−TB cases shoot up.** The number of people with extreme−drug resistant tuberculosis (XDR−TB) has more than quadrupled in the Western Cape, South Africa, in the past three months, provincial health department figures show. Also, the Brooklyn Chest TB Hospital has no room for more patients. It has 22 beds in the isolation wards to treat XDR−TB cases. This comes as the City of Cape Town has drawn up contingency plans in the event of an XDR−TB outbreak. Since March, 45 XDR−TB cases have been notified in the province. Eight people have died, according to department figures. In March, there were 10 known XDR−TB cases in the province. XDR−TB, which withstands first−and second−line antibiotic treatment, is almost impossible to treat. It has killed 290 patients nationwide.
Source: http://www.int.iol.co.za/index.php?set_id=1&click_id=125&art_id=vn20070621011130371C820336

[Return to top]

Government Sector

30. *June 28, Associated Press* — **Ohio courthouse evacuated after mercury spill.** Authorities say the Morrow County courthouse in central Ohio is to remain closed Thursday, June 28, following Wednesday's evacuation due to a mercury spill. Sheriff Steve Brenneman says the poisonous substance was found in hallways on two floors of the building. Most of the building was slowly evacuated yesterday afternoon and people were asked to remove their shoes so they could be checked for contamination. Brenneman says the source of the mercury is unknown, and there are no reports of people being sickened.
Source: http://www.local12.com/news/state/story.aspx?content_id=e6f098a5−5489−42e0−b23d−56ce7489316a

[Return to top]

Emergency Services Sector

31. *June 27, Colorado Springs Gazette (CO)* — **Delay turns drill into a disaster.** A mass casualty drill Wednesday, June 27, turned into a minor disaster because fire trucks and ambulances couldn’t reach “injured” survivors of a mock plane crash. American Medical Response (AMR) ambulances and Colorado Springs, CO, firefighters didn’t reach the “crash” scene on Peterson Air Force Base until an hour after the drill began. Doug McIntyre, a paramedic and disaster coordinator for AMR, said the delay was due to an escort’s failing to accompany the five ambulances and firefighters taking part in the drill through a security gate. The main problem, said Cindy Litteral, Peterson’s deputy fire chief, was miscommunication. John McGinley, assistant director of operations and maintenance at Colorado Springs Airport, which shares runways with Peterson, said part of the delay in getting ambulances to the site was due to having the drill by an active airfield and the need for trucks to drive along perimeter roads. Despite miscommunications between the six military and civilian agencies involved, organizers termed the drill a success that provided lessons for avoiding future mistakes and working together.

Source: http://www.gazette.com/articles/drill_24166___article.html/m cintyre_crash.html

[Return to top]

Information Technology and Telecommunications Sector

32. *June 28, CNET News* — **Gartner: Businesses should be wary of iPhone.** Analyst Gartner claims the iPhone could "punch a hole" through corporate security systems if workers are allowed to use the phone for work purposes. IT departments should be extremely wary of allowing employees to use Apple's mobile handset because it does not contain the necessary functionality to comply with basic corporate security, analysts warned in a research note released on Thursday, June 28. The iPhone will be launched in the U.S. on Friday. Gartner lists the following reasons to steer clear of the iPhone for now: a) Lack of support from major mobile device management suites and mobile−security suites; b) Lack of support from major business mobile e−mail solution providers; c) An operating system platform that is not licensed to alternative−hardware suppliers, meaning there are limited backup options; d) Feature deficiencies that would increase support costs; e) Currently available from only one operator in the U.S.; f) An unproven device from a vendor that has never built an enterprise−class mobile device; g) The high price of the device, which starts at $500; H) A clear statement by Apple that it is focused on consumer rather than enterprise.
Source: http://news.com.com/Gartner+Businesses+should+be+wary+of+iPhone/2100−7350_3−6193856.html?tag=nefd.top

33. *June 28, Sophos* — **Harry Potter worm targets USB memory drives.** With just weeks remaining until the release of the last ever Harry Potter novel, and the imminent premiere of the fifth movie in the franchise, Sophos has warned of a new computer worm exploiting Potter−mania around the world. The W32/Hairy−A worm spreads by copying itself onto USB memory sticks, posing as a copy of the eagerly−anticipated novel "Harry Potter and the Deathly Hallows." Windows users who allow affected flash drives to "autorun" are automatically infected by the worm when it is attached to their PC. A file called HarryPotter−TheDeathlyHallows.doc can be found in the root directory of infected USB drives. Inside the Word document file is the simple phrase "Harry Potter is dead."
Source: http://www.sophos.com/pressoffice/news/articles/2007/06/hair y.html

34. *June 27, InformationWeek* — **Hackers take over MySpace pages to build bots.** Internet Storm Center researchers are warning users that drive−by exploits have been embedded in a few dozen legitimate MySpace pages. Johannes Ullrich, chief technology officer with the Internet Storm Center, told InformationWeek that the malicious code that's embedded in the Webpages installs the FluxBot, a dangerous new bot. Since the bot doesn't have a central command and instead relies on a complex set of ever−changing networks of proxy servers, Ullrich said it's extremely difficult to shut it down or cleanse it off an infected system. Ullrich explained that the embedded malicious code tries to exploit an old Microsoft Internet Explorer bug that was patched mid−2006. If that bug lets in the exploit, then the FluxBot is downloaded. "The IE hole is not particularly dangerous at this point, but quite a few people still got hit," he added. "I guess there are a lot of people out there with unpatched versions of Internet Explorer." Ullrich also noted that while MySpace isn't a new target for hackers, it's an increasingly popular one.

Source: http://www.informationweek.com/security/showArticle.jhtml;jsessionid=B50NC0JHNDDKAQSNDLRSKHSCJUNN2JVN?articleID=20000112 2

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.
[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non−commercial publication intended to educate and inform